Host Mitigation Package (HMP)

Introduction

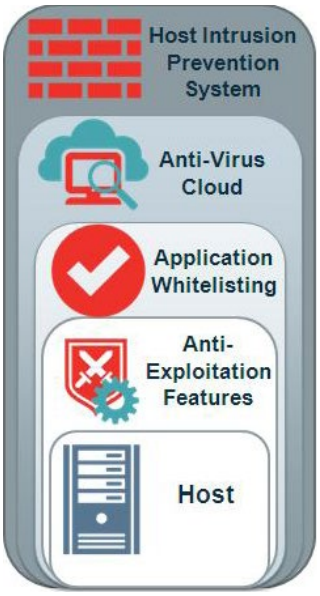
Our adversaries' command of modern technology and proficiency in exploiting vulnerabilities limits our ability to deploy computer network defensive capabilities in today's environment. The constant introduction of new applications and platforms – coupled with the exponential increase in computing power – creates an enormous challenge for system administrators to adequately defend against malicious activity taking place on the network. Detection of any new threat is often discovered only after data has been exfiltrated or other artifacts of an attack have been identified.

The normal response to any successful attack is to develop and deploy tools that will oppose that specific threat. However, that approach is reactionary in nature and does nothing to counter sophisticated adversaries that can easily overcome this type of signature-based response strategy by making simple modifications to their code. A proactive way forward that focuses on prevention rather than reaction is needed. As such, the Host Mitigations Package (HMP) is designed to aid organizations and system administrators in hardening their host systems.

Host Mitigations Package Overview

Most organizations tend to focus on securing the larger network. Devices such as firewalls, routers, and Intrusion Detection and Prevention systems get most of the attention from network administrators. Although securing the network is vital, hardening host systems is just as essential and deserves the same level of consideration. The Department of Defense (DoD) is working to address emerging host threats by implementing capabilities like the SANS Top 20 Security Controls. However, this effort is focused on a comprehensive program regarding host hardening.

HMP was constructed in order to corral the many disparate security controls into one package. The HMP supports the defense-in-depth strategy in which multiple layers of security controls are placed throughout a host. Any single layer of defense will most certainly contain



gaps that could be exploited by an adversary. A series of different security defenses residing in a single host should be used to cover the gaps in other layers. The intent of HMP is to not only prevent security breaches, but also to buy an organization time to detect and respond to an attack. As such, an adversary that is not stopped cold will have to work harder and longer, thus reducing and mitigating the consequences of a breach. The HMP uses an efficient combination of operational tools designed to provide a layered defense against the most common and most effective techniques utilized by hostile actors.

This package was designed to implement existing commercial software to provide high gains at a low resource cost to increase overall system security. The HMP is modular and can be tailored to fit customer needs. The tools included in the package are: system configurations, freely available commercial software, or Government enterprise-licensed software, all of which are freely available for immediate download. Additional information for these tools is provided in the references below. System administrators should expect about two weeks to tune the software for optimal performance across their network. The HMP suite of tools works with the standard baseline of Microsoft® Windows XP®, Windows 7®, or Windows 8® operating systems[1].

The HMP includes the following capabilities:

1. Application Whitelisting
2. Anti-Exploitation Features
3. Anti-Virus Cloud Lookup
4. Host Intrusion Prevention System

Application Whitelisting

All applications can introduce unknown and unacceptable security risks to any host or network. Application Whitelisting (AWL) is a proactive security technique where only a limited set of approved programs is allowed to run. By default, all other programs – including most malware – are blocked from running. AWL prevents the use of unauthorized applications, thereby limiting the attack surface to only security risks that the organization has chosen to accept. In contrast, the standard policy enforced by most operating systems allows all users to download and run any program they choose.

AWL is only one layer in the defense-in-depth strategy and is not a replacement for traditional security software such as anti-virus (AV) and host firewalls. For an AWL solution to be effective, all executable code must be blocked by default so only approved programs can run. Users must not be allowed to modify the files that are allowed to run. AWL enables administrators, not users, to decide which programs are allowed to execute.

AWL Advantages:

1. Blocks most current malware
2. Prevents use of unauthorized applications
3. Does not require daily definition updates
4. Requires administrator installation and approval of new applications

Anti-Exploitation Features

An anti-exploitation feature provides protection against exploits in a broad, generic manner. This is in contrast to AV or signature-based detection, which looks for specific known-bad pieces of code or malicious files. Anti-exploitation features are especially effective against common attacks meant for mass infection, such as drive-by download sites, malicious iframes, and phishing campaigns. They also help mitigate zero-day vulnerabilities - previously unknown vulnerabilities with no available patches or fixes.

One example of an anti-exploitation feature is Microsoft's Enhanced Mitigation Experience Toolkit (EMET)®, which is available for Windows systems[2]. It is a host-based application that hooks into processes and watches for common memory exploitation techniques like buffer overflow attacks. These common attacks use vulnerabilities present in un-patched versions of Adobe Reader®, Flash Player®, and other frequently used applications[3]. When EMET detects an exploit attempt, it promptly kills the targeted process, logs the attempt, and notifies the user that it has shut down the application.

EMET is a free application and can be deployed using typical enterprise deployment methods. Once deployed, maintenance is very low although some time must be taken to monitor and resolve possible compatibility issues that could arise. The links in the reference section provide guidance on effective deployment and maintenance strategies.

EMET Advantages:

1. Stops attacks at the exploit stage before any payload can be delivered
2. Stops common drive-by download attacks
3. Requires the adversary to change their exploits to bypass it, increasing their costs and lowering success rates
4. Simple to deploy and easy to maintain
5. Adds another layer to a defense-in-depth strategy at a very low cost

Anti-Virus Cloud Lookup

The majority of technologies currently in use to detect malicious activity rely on signatures of "known-bad" activity or files. This approach is very easily defeated by small modifications to malicious files or through innovative new techniques. Recent advances in AV technologies – by vendors such as McAfee® and Symantec™ – leverage a "cloud lookup" capability in which files can be referenced against a global reputation database to discover new potentially malicious activity and report to system administrators for follow-on

remediation[4]. This capability is alternatively referred to as File Reputation Lookup and Cloud Heuristics. Additionally, McAfee and Symantec have proprietary names for their capabilities: GTI® and Insight™, respectively[5].

AV applications get the most up-to-date intelligence about suspicious files or activities by reaching back into the cloud. This reach back provides near real-time protection of the endpoint against new and emerging threats and improves security posture of the GIG. AV Cloud lookup can serve as protection from new malicious files until they are incorporated into enterprise deployed signature files. For example, GTI detects specific instances of malware as opposed to classes of malware, which significantly reduces the chances of generating false-positive detections. This Cloud capability provides protection to the hosts above and beyond what is offered by existing signature files.

AV Cloud Lookup Advantages

1. Protection against newly discovered malware can be initiated within seconds versus the hours or days required for updating host detection via signature files
2. Provides mechanisms for better control over every file entering the network, helping to stop malware execution, which is one of the most pressing network defense challenges
3. Better positions an enterprise to respond to fast moving attacks that could hinder operations across the non-classified network
4. Has a lower false positive rate than existing .DAT files
5. Provides 10% to 30% better detection than signature DAT files alone, according to preliminary testing

Host Intrusion Prevention System

A Host Intrusion Prevention System (HIPS) is a valuable component used to defend computer host integrity. In enterprise deployments, a HIPS is centrally managed, and system administrators push policies and rules down to the individual hosts. Alerts of malicious or abnormal activity on the hosts are pushed back up to the management system where they can be correlated and acted upon. The HIPS policy can be set to log and/or block the malicious or suspicious activity. A HIPS typically includes four different technologies: a host firewall, a registry monitor, a file integrity monitor, and a process/application behavior monitor.

One HIPS example is the Host Based Security System (HBSS), the DoD commercial-off-the-shelf suite of software applications used to monitor, detect, and counter attacks against DoD computer networks and systems. The Enterprise-wide Information Assurance and Computer Network Defense Solutions Steering Group sponsored the acquisition of HBSS for use within the DoD Enterprise Network. This enterprise solution is installed throughout the DoD enterprise.

HBSS is centered on McAfee's ePolicy Orchestrator® (McAfee ePO™) management engine and consists of several point products[6]. McAfee point products include the Host Intrusion Prevention System, Policy Auditor, Assets Baseline Module, Rogue System Detection, Device Control Module, and the Asset Publishing Service.

HBSS Advantages

1. Capability to block unknown intrusion signatures and restrict unauthorized services and applications
2. Addresses system baseline configurations and reacts to changes in the Operations environment
3. Provides real-time detection of new hosts attaching to the network
4. Ensures application patching compliance

Summary

Malicious attacks against DoD networks are increasing every year. In order to help system administrators combat these attacks, the Information Assurance

Directorate has developed a mitigations package that focuses entirely on the host. This Host Mitigations Package assembles a series of tools that share overlapping security boundaries in order to provide defense-in-depth protection against an attack. These tools and configurations are easy to use and deploy with little to no cost.

References

Anti-Exploitation:
http://support.microsoft.com/kb/2458544

Application Whitelisting:
www.iad.gov/iad/cgs/cgs.cfm
(select Manageable Network Plan at the bottom and see the Executable Content Restrictions section, pg.24)

AV Cloud:
McAfee GTI – **http://www.mcafee.com/us/threat-center/technology/gti-reputation-technologies.aspx**

Symantec Insight – **http://www.symantec.com/reputation-based-security**

HIPS:
McAfee HIPS product – **www.mcafee.com/us/products/host-ips-for-desktop.aspx**

Symantec's Critical System Protection – **www.symantec.com/critical-system-protection**

Contact Information

Industry Inquiries: 410-854-6091

USG/IC Client Advocates: 410-854-4790

DoD/Military/COCOM Client Advocates: 410-854-4200

General Inquiries: **niasc@nsa.gov**